Configuratievoorbeeld voor beveiligde externe telefoonservices

Inhoud

Inleiding

Dit document beschrijft hoe u de Secure Externe Telefoonservice kunt configureren. Deze configuratie kan met elke service van derden werken, maar voor demonstratie gebruikt dit document een externe Cisco Unified Communications Manager (CUCM)-server.

Bijgedragen door Jose Villalobos, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- CUCM
- CUCS-certificaten
- Telefonische services

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- CUCM 10.5.X/CUCM 11.X
- Session Client Control Protocol (SCCP) en Session Initiation Protocol (SIP)-telefoons (registreren met CUCM
- Het lab gebruikt alternatieve (SAN)-certificaten.
- Externe folder zal op SAN certs staan.
- Voor alle systemen in dit voorbeeld zal de certificaatinstantie (CA) hetzelfde zijn, alle certs die worden gebruikt CA-teken.
- Domain Name Server (DNS) en Network Time Protocol (NTP) moet worden ingesteld en werken.

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van elke verandering begrijpt.

Verwante producten

Dit document kan ook met deze hardware- en softwareversies worden gebruikt:

- CUCM 9.X/10.X/11.X

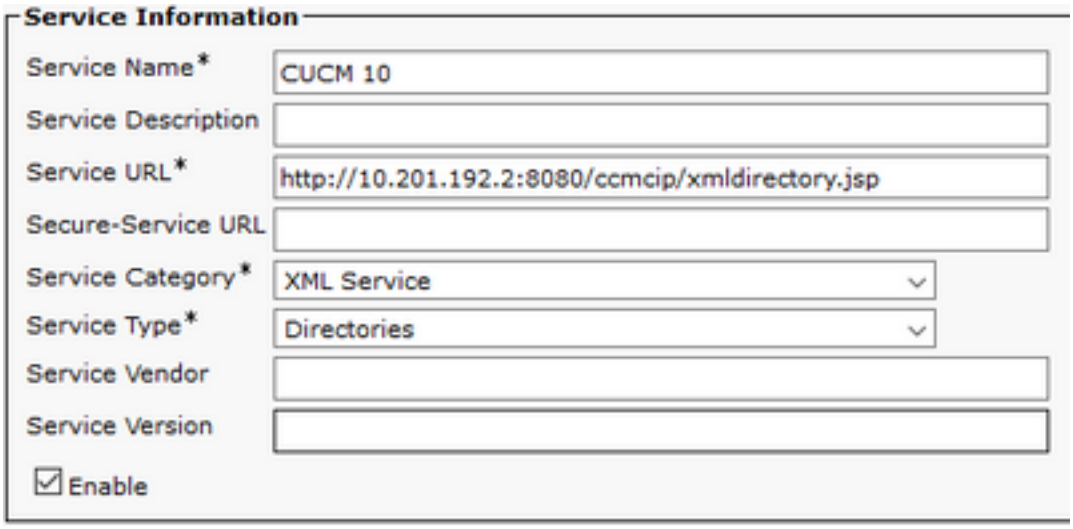
Configuratiestappen

Stap 1. Stel de URL in het systeem in.

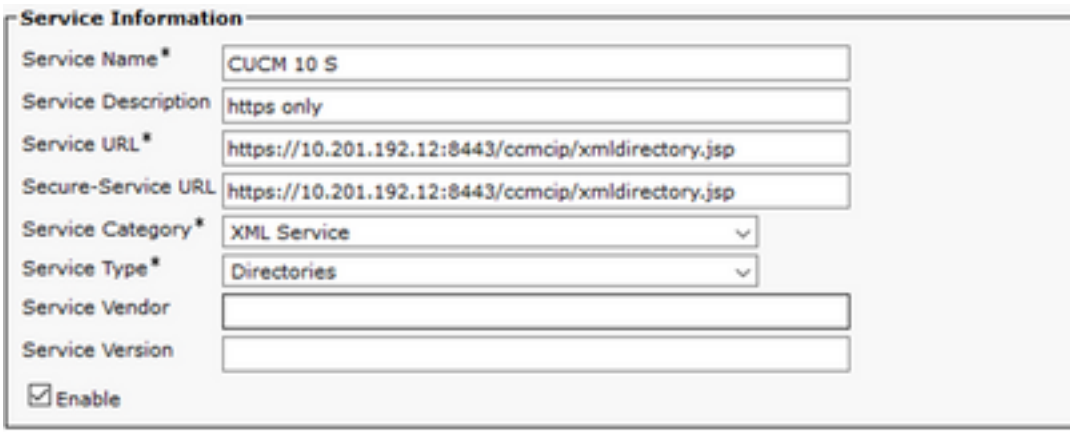
Setup Hyper-Text Transfer Protocol (HTTP) en Hypertext Transfer Protocol (HTTPS) als bewijs van concepten. Het uiteindelijke idee is alleen Secure HTTP Traffic Engineering te gebruiken.

Navigeren in naar **apparaat> Apparaatinstellingen> Telefonische service> Toevoegen nieuwe software**

alleen HTTP



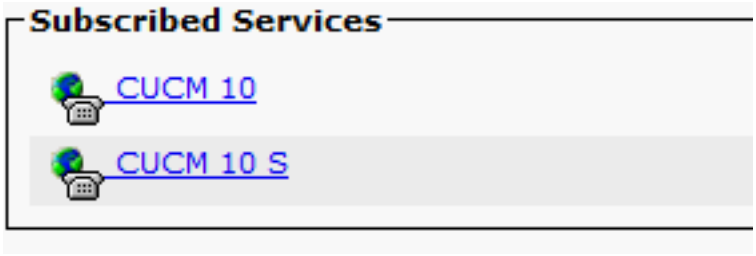
Alleen HTTPS



Waarschuwing: als u de controle voor **Enterprise Subscriber** toevoegt**,** kan stap twee worden overgeslagen. Maar deze verandering stelt alle telefoons opnieuw in, zodat je de mogelijke impact begrijpt.

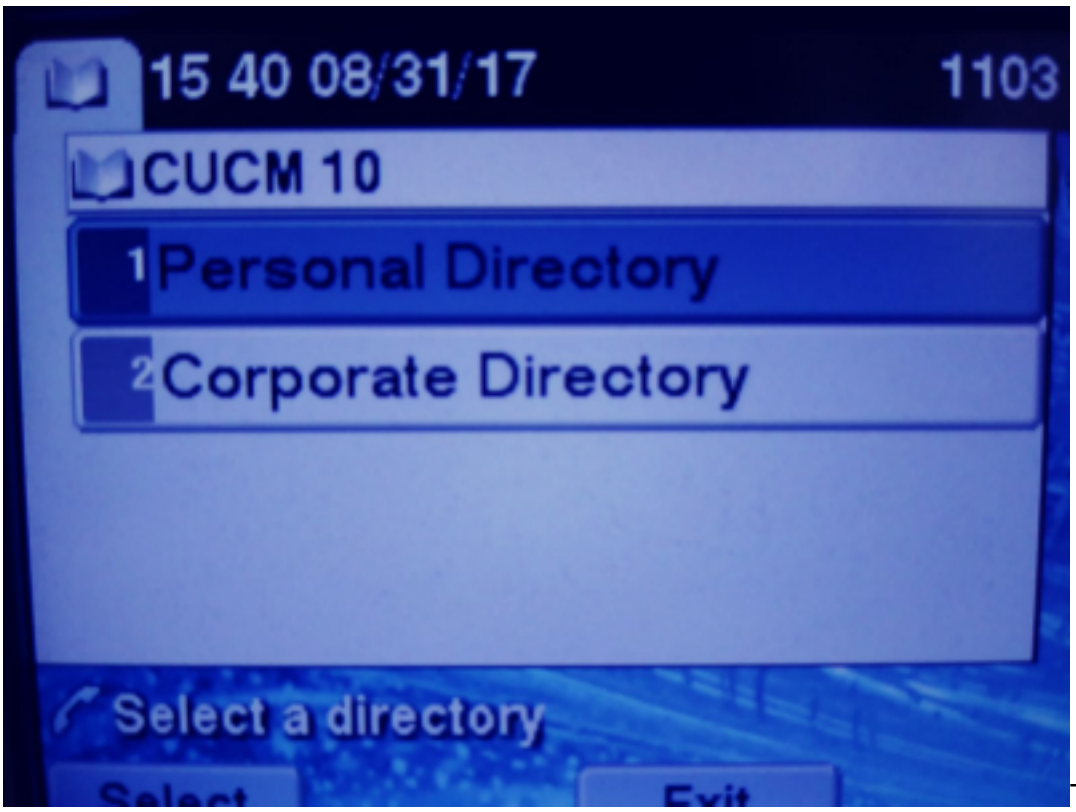
Stap 2. Subscriber de telefoons aan de services.

Inschakelen op **apparaat>Telefoon>Subscriber/UnSubscriber-service.**



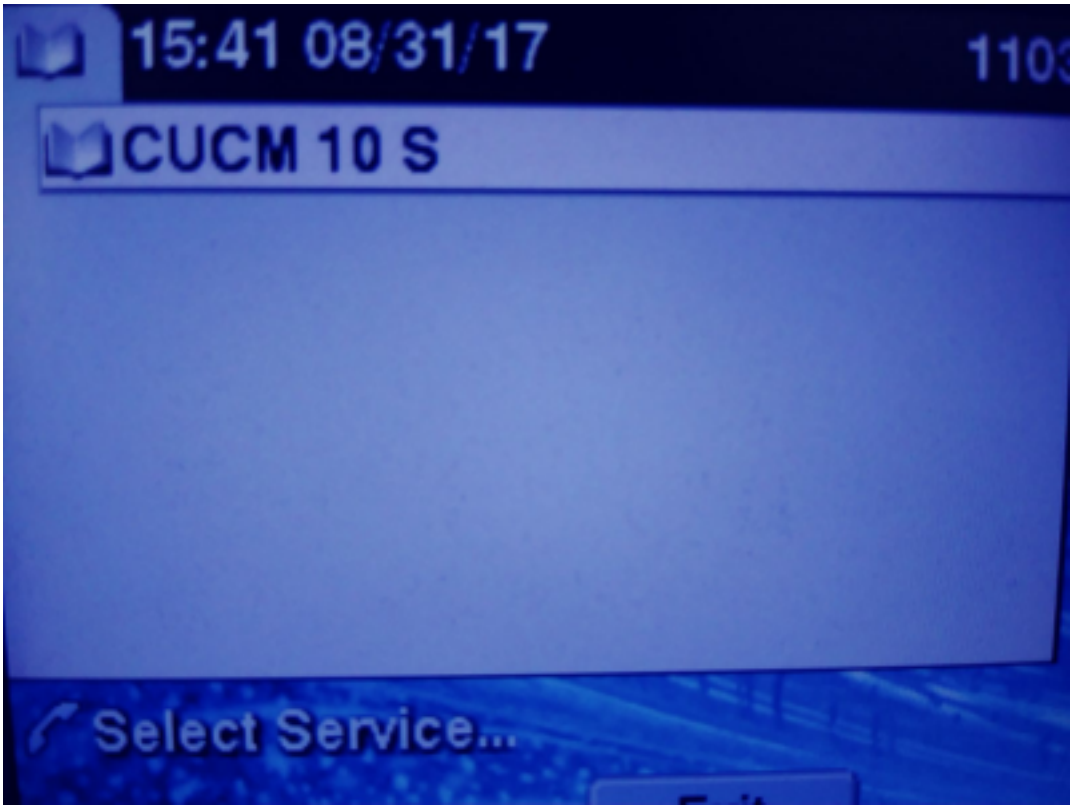
Op dit punt, als de toepassing HTTP aanbiedt, moet je de service kunnen bereiken, maar https is nog niet omhoog.

HTTP



TTP

HTTPS



HTTPS zal een "Host niet gevonden" fout vanwege het feit tonen, kan de TVS-dienst dit voor de telefoon niet echt verklaren.

Stap 3. Upload de externe servicecertificaten naar het CUCM.

Upload de Externe Dienst als **Tomcat alleen maar vertrouwt**. Zorg ervoor dat de services op alle knooppunten zijn teruggezet.

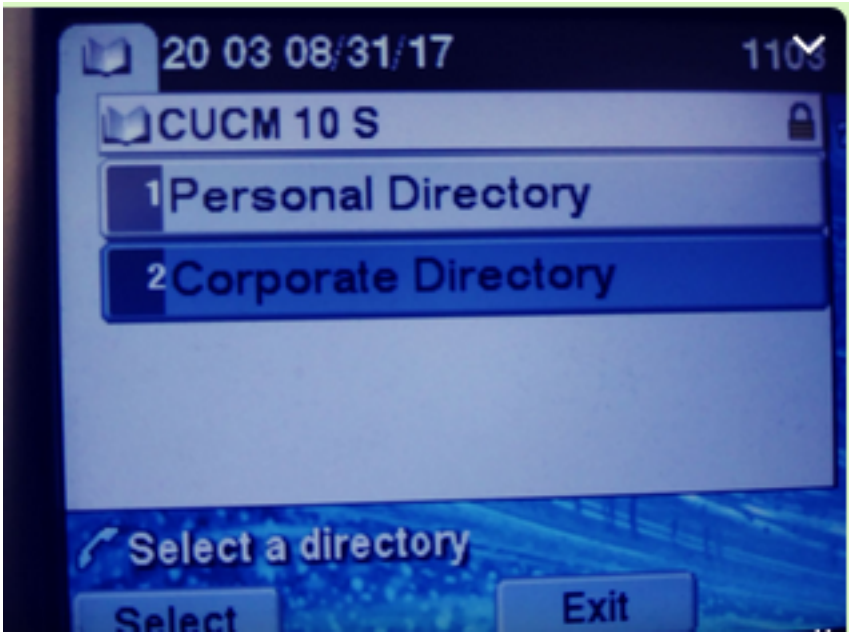
Dit type certs wordt niet opgeslagen op de telefoon, maar de telefoon moet met de TVS-service controleren om te zien of er een HTTPS-verbinding is.

Navigeren in naar **OS-beheerder> certificaatuploaden.**

Van SSH stelt u de CUCM Tomcat-service op alle knooppunten in.

```
admin:utils service restart Cisco Tomcat
Do not press Ctrl+C while the service is restarting. If the service has not rest
arted properly, execute the same command again.
Service Manager is running
```

Na deze stappen moeten telefoons zonder problemen toegang hebben tot de HTTPS-service



Vaak gestelde vragen (FAQ)

Nadat certificaten zijn uitgewisseld, faalt HTTPS nog steeds met "host not found".

-Controleer het knooppunt waar u het register aanwijst en zorg ervoor dat u het certificaat van derden voor het knooppunt ziet.

- Zet de tekst op het specifieke knooppunt terug.

-Controleer DNS, en zorg ervoor dat de gemeenschappelijke naam (GN) van het certificaat kan worden opgelost.

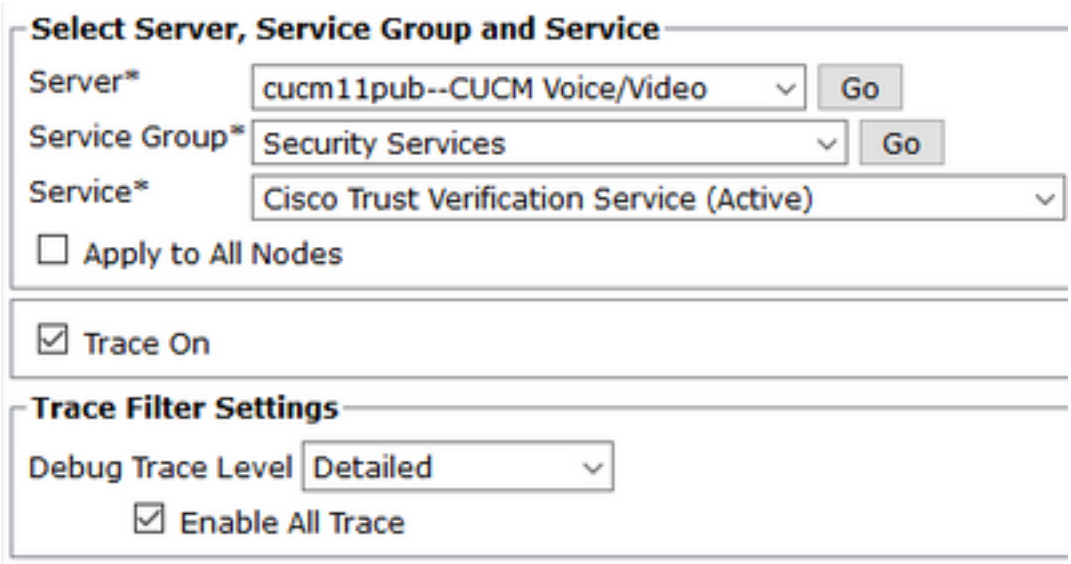
Probleemoplossing

Verzamel CUCM TVS-logbestanden om u goede informatie te geven

Navigatie naar **RTMT>Systeem>Zoeken en loggen Centraal > Logbestanden verzamelen**

> Opmerking: Verzamel logbestanden vanaf alle knooppunten en zorg ervoor dat de TVS-logbestanden op details zijn ingesteld.

TVS-bestanden ingesteld op gedetailleerd



Voorbeeld overtrekken

```
11:17:38.291 |   debug CTVSChangeNotifyServer::ProcessChangeNotification () -
CDBString=<msg><type>DBL</type><table>certificate</table><tableid>46</tableid><action>I</action>
<user>repl</user><time>1504203458</time><new><cdrserver>2</cdrserver><cdrtime>1504203457</cdrtim
e><pkid>e6148ee3-3eb5-e955-fa56-
2baa538a88fb</pkid><servername>cucm11pub</servername><subjectname>CN=10.201.192.12,OU=RCH,O=Cisc
o,L=RCH,ST=Tx,C=US</subjectname><issuername>CN=pablogon-
CA,DC=rcdncollab,DC=com</issuername><serialnumber>3d00000008230ded92f687ec03000000000008</serial
number><certificate></certificate><ipv4address>10.201.192.13</ipv4address><ipv6address></ipv6add
ress><timetolive>NULL</timetolive><tkcertificatedistribution>1</tkcertificatedistribution><ifx_r
eplcheck>6460504654345273346</ifx_replcheck></new></msg>
11:17:38.291 |   debug CTVSChangeNotifyServer::ProcessChangeNotification () - Database table
"certificate" has been changed
11:17:38.291 |   debug CTVSChangeNotifyServer::ProcessChangeNotification () - Looking up the
roles for
11:17:38.291 |   debug Pkid : fead9987-66b5-498f-4e41-c695c54fac98
11:17:38.291 |   debug CTVSChangeNotifyServer::ProcessThreadProc () - Waiting for DBChange
Notification
11:17:38.300 |   debug CTVSChangeNotifyServer::ProcessThreadProc () - DBChange Notification
received
11:17:38.300 |   debug CTVSChangeNotifyServer::ProcessChangeNotification () -
CDBString=<msg><type>DBL</type><table>certificatetrustrolemap</table><tableid>50</tableid><actio
n>I</action><user>repl</user><time>1504203458</time><new><cdrserver>2</cdrserver><cdrtime>150420
3457</cdrtime><pkid>5ae6e1d2-63a2-4590-bf40-1954bfa79a2d</pkid><fkcertificate>e6148ee3-3eb5-
e955-fa56-
2baa538a88fb</fkcertificate><tktrustrole>7</tktrustrole><ifx_replcheck>6460504654345273346</ifx_
replcheck></new></msg>
11:17:38.300 |   debug CTVSChangeNotifyServer::ProcessChangeNotification () - Database table
"certificatetrustrolemap" has been changed
11:17:38.300 |   debug CTVSChangeNotifyServer::ProcessThreadProc () - Waiting for DBChange
Notification
11:17:46.811 |   debug updateLocalDBCache : Refreshing the local DB certificate cache
11:34:00.131 |   debug Return value after polling is 1
11:34:00.131 |   debug FD_ISSET i=0, SockServ=14

11:34:00.131 |   debug Accepted TCP connection from socket 0x00000014
```